### TRAITE COOPERATION EN MATIERE

**PCT** 

REC'D 0 7 JUN 2004

PCT

### RAPPORT D'EXAMEN PRELIMINAIRE INTERNATIONAL

(article 36 et règle 70 du PCT)

Référence du dossier du déposant ou du mandataire			POUR SUITE A DONNER voir la notification de transmission du rapport d'examen préliminaire international (formulaire PCT/IPEA/416)							
Demande internationale No. PCT/IB 03/02425			Date du dépôt internations 10.06.2003	al (jour/mois/année)	Date de priorité (jour/mols/année) 12.06.2002					
Classificat	ion inter	nationale des brevets (CIE	3) ou à la fois classification r	nationale et CIB						
	Classification internationale des brevets (CIB) ou à la fois classification nationale et CIB H04L9/08									
Déposant										
NAGRACARD SA et al.										
Le présent rapport d'examen préliminaire international, établi par l'administaration chargée de l'examen préliminaire international, est transmis au déposant conformément à l'article 36.										
2. Ce	2. Ce RAPPORT comprend 5 feuilles, y compris la présente feuille de couverture.									
	and the state of t									
Се	s anne	xes comprennent feuil	lles.							
3. Le	présen	it rapport contient des i	ndications et les pages co	orrespondantes relati	ves aux points sulvants :					
1	$\boxtimes$	Base de l'opinion								
11		Priorité								
111		Absence de formulati possibilité d'application	ion d'opinion quant à la no on industrielle	ouveauté, l'activité inv	ventive et la					
IV	IV Absence d'unité de l'invention									
V	The second distribution of the second distributi									
VI		Certains documents	cités							
VI		Irrégularités dans la c	demande internationale							
1	VIII  Observations relatives à la demande internationale									
Date de présentation de la demande d'examen préliminaire internationale			men préliminaire	Date d'achèvement du	ı présent rapport					
20.12.2003				07.06.2004						
Nom et adresse postale de l'adminstration chargée de l'examen préliminaire international				Fonctionnaire autorisé	Andrews Princeton . E.					
Office européen des brevets - P.B. 5818 Patentlaan 2				Holper, G						
	ル Fa	51. +31 70 340 - 2040 Tx: 3 ax: +31 70 340 - 3016	31 65 <b>1 epo ni</b>	N° de téléphone +31 7	70 340-2304					

## RAPPORT D'EXAMEN PRÉLIMINAIRE INTERNATIONAL

Demande internationale nº

PCT/IB 03/02425

I. Bas	e du	rapp	ort
--------	------	------	-----

1. En ce qui concerne les éléments de la demande internationale (les feuilles de remplacement qui ont été remises à l'office récepteur en réponse à une invitation faite conformément à l'article 14 sont considérées, dans le présent rapport, comme "initialement déposées" et ne sont pas jointes en annexe au rapport puisqu'elles ne contiennent pas de modifications (règles 70.16 et 70.17)): **Description, Pages** 1-13 telles qu'initialement déposées Revendications, No. 1-16 telles qu'initialement déposées Dessins, Feuilles 1/2-2/2 telles qu'initialement déposées 2. En ce qui concerne la langue, tous les éléments indiqués ci-dessus étaient à la disposition de l'administration ou lui ont été remis dans la langue dans laquelle la demande internationale a été déposée, sauf indication contraire donnée sous ce point. Ces éléments étaient à la disposition de l'administration ou lui ont été remis dans la langue suivante: ,qui est: la langue d'une traduction remise aux fins de la recherche internationale (selon la règle 23.1(b)). la langue de publication de la demande internationale (selon la règle 48.3(b)). la langue de la traduction remise aux fins de l'examen préliminaire internationale (selon la règle 55.2 ou 55.3). 3. En ce qui concerne les séquences de nucléotides ou d'acide aminésdivulguées dans la demande internationale (le cas échéant), l'examen préliminaire internationale a été effectué sur la base du listage des séquences: contenu dans la demande internationale, sous forme écrite. déposé avec la demande internationale, sous forme déchiffrable par ordinateur. ☐ remis ultérieurement à l'administration, sous forme écrite. remis ultérieurement à l'administration, sous forme déchiffrable par ordinateur. La déclaration, selon laquelle le listage des séquences par écrit et fourni ultérieurement ne va pas au-delà de la divulgation faite dans la demande telle que déposée, a été fournie. La déclaration, selon laquelle les informations enregistrées sous déchiffrable par ordinateur sont identiques à celles du listages des séquences Présenté par écrit, a été fournie. 4. Les modifications ont entraîné l'annulation : ☐ de la description, pages: des revendications, nos:

feuilles:

des dessins.

#### RAPPORT D'EXAMEN PRÉLIMINAIRE INTERNATIONAL

Demande internationale nº

1-16

PCT/IB 03/02425

5. 🗆	présent rapport a été formulé abstraction faite (de certaines) des modifications, qui ont été consi mme allant au-delà de l'exposé de l'invention tel qu'il a été déposé, comme il est indiqué ci-après .2(c)) :	dérées (règle
------	--	------------------

(Toute feuille de remplacement comportant des modifications de cette nature doit être indiquée au point 1 et annexée au présent rapport.)

- 6. Observations complémentaires, le cas échéant :
- V. Déclaration motivée selon l'article 35(2) quant à la nouveauté, l'activité inventive et la possibilité d'application industrielle; citations et explications à l'appui de cette déclaration
- 1. Déclaration

Nouveauté Oui: Revendications

Non: Revendications

Activité inventive Oui: Revendications 1-16

Non: Revendications

Possibilité d'application industrielle Oui: Revendications 1-16

Non: Revendications

2. Citations et explications

voir feuille séparée

## RAPPORT D'EXAMEN Demande internationale n° PCT/IB03/02425 PRELIMINAIRE INTERNATIONAL - FEUILLE SEPAREE

#### Concernant le point V

Déclaration motivée selon l'article 35(2) quant à la nouveauté, l'activité inventive et la possibilité d'application industrielle; citations et explications à l'appui de cette déclaration

Il est fait référence au document suivant:

D1: WO 97/38530 (DIGCO)

La présente demande concerne un procédé d'échange sécurisé d'informations localement connectés entre eux ainsi qu'un récepteur pour la mise en oeuvre du dit procédé.

L'état de la technique le plus proche est illustré par D1 qui divulgue un procédé d'échange sécurisé d'informations entre un récepteur et un module de sécurité, les deux dispositifs étant localement connectés. Le récepteur comporte une clé publique tandis que le module de sécurité comporte une clé privée correspondante. Le procédé sert à échanger une clé de session aléatoire chiffrée par la clé publique.

Problème dans l'état de la technique: la clé de session peut être imposée par un intrus qui utiliserait ainsi une lacune de sécurité du procédé.

Selon la revendication 1 ce problème est résolu par les étapes consistant à générer un nombre aléatoire différent dans chaque dispositif, chiffrer ce nombre par la première respectivement la seconde clé de la paire de clés, transmettre le nombre chiffré à l'autre dispositif, déchiffrer les nombres chiffrés dans chaque dispositif et combiner les dispositif et combiner les dispositifs pour générer une clé de session utilisée pour l'échange de données entre les deux dispositifs.

Un procédé basé sur le chiffrage de deux nombres aléatoires chiffrés par deux clés différentes de la même paire de clés n'est pas connu ni suggéré par l'état de la technique.

La revendication 1 remplit donc les critères de nouveauté et d'activité inventive de l'article 33(2) et (3) PCT.

Le récepteur selon la revendication 15 est arrangé pour la mise en oeuvre du procédé selon la revendication 1 et remplit donc aussi les critères de nouveauté et d'activité

**BEST AVAILABLE COPY** 

# RAPPORT D'EXAMEN Demande internationale n° PCT/IB03/02425 PRELIMINAIRE INTERNATIONAL - FEUILLE SEPAREE

inventive.

Les caractéristiques supplémentaires des revendications dépendantes 2-14 et 16 définissent des détails de réalisation de sorte que ces revendications sont aussi nouvelles et inventives.

Les procédés et récepteurs revendiqués présentent la possibilité d'activité industrielle.

BEST AVAILABLE COPY